

Patent claims

1. A method for putting into operation a processor smart card for a network for communication, preferably a GSM network, wherein the card user must identify himself with respect to the processor smart card (SIM) by a personal identification number, characterized in that
 - for execution control of the first use, the processor smart card is first provided by the card manufacturer or card personalizer with an additional application, preferably using the SIM Application Toolkit, which prevents its use in the network, instead allowing only local use by means of a card reader or card terminal, preferably a mobile phone device, and
 - upon the first use of the processor smart card, the application outputs without a further check of a secret number a display signal for the first use and a request for confirmation, and
 - after receiving a confirmation signal the additional application is deactivated or its execution so changed that upon the next use of the card a display signal is outputted to indicate that the card has already been put into operation and the use of the processor smart card in the network is enabled.
2. A method according to claim 1, characterized in that a personal identification number previously defined, preferably by the card manufacturer or card personalizer, must be inputted for activating the additional application.
3. A method according to claim 1 or 2, characterized in that the entry of a personal identification number (PIN) and/or a secret number (PUK) for changing or unblocking the personal identification number (PIN) is requested after the first use of the card and prior to the deactivation or change of state of the additional application.
4. A method according to any of claims 1 to 3, characterized in that some or all personal identification numbers on the card were already personalized on the processor smart card by the card manufacturer and said numbers are indicated

upon the first use for later use on the card reader or card terminal, preferably a mobile phone device.

- Sub 91
5. A method according to any of claims 1 to 4, characterized in that some or all personal identification numbers on the card are set by a random-number generator built into the card and said numbers are indicated during the first use on the card reader or card terminal, preferably a mobile phone device.
 6. A method according to any of claims 1 to 5, characterized in that some or all personal identification numbers are combined for transmission to the network, preferably in encrypted form via a data channel, and sent immediately or at a later time to a central place at the network operator or network service provider.
 7. A method according to any of claims 1 to 6, characterized in that the secret numbers to be defined at the first putting into operation are used not for the purpose of protecting the network application but for protecting an additional application, preferably a SIM Application Toolkit application, on the SIM card.
 8. A method according to any of claims 1 to 7, characterized in that information on the first use of the processor smart card and on the personal identification numbers is outputted or inputted via the hearing or speaking devices of the card reader, the card terminal or preferably the mobile phone device.
 9. A smart card having a microprocessor (μP), a memory area (M) and an interface (S) each connected with the microprocessor (μP), characterized by a memory area (A) where an application for the execution control of the first use of the smart card is stored, and a secret memory area (Mg) where data on said application are stored in protected fashion.

0906450.01550